Mediterranean Journal of Basic and Applied Sciences (MJBAS)
Volume 10, Issue 2, Pages 48-66, April-June 2026

Assessment of Consumer Cybersecurity Awareness, Fraud Vulnerability, and Trust in E-Commerce Platforms: Toward a Proposed Machine Learning-Based Detection Framework for Order Scams and Payment Fraud

Lester Bulay[1*], Redjan Phil S. Visitacion[2], Jazhtene D. Orale[3], Alyssa Mae C. Rodriguez[4], Johny M. Roldan[5], Arlyn Kaye Allona D. Baluyos[6], Micah Colleine Pantua[7], Frisel Lagane[8], Jhon Peter U. Codilla[9], Alexander Pepito[10], Mark Cyril Sumoroy[11], Kurt Russell Dolalas[12] & Ginbert A. Fernandez[13]

[1-13]*Department of Information Technology, College of Engineering and Technology, University of Science and Technology of Southern Philippines – Oroquieta Campus, Oroquieta City, Misamis Occidental, 7207, Philippines.*
Corresponding Author (Lester Bulay) Email: lesterbulay18@gmail.com[*]

DOI: https://doi.org/10.46382/mjbas.2026.10204

Copyright © 2026 Lester Bulay et al. This is an open-access article distributed under the terms of the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original author and source are credited.

Article Received: 22 February 2026 *Article Accepted: 24 April 2026* *Article Published: 26 April 2026*

ABSTRACT

With the rapid rise of e-commerce platforms, the risk of order scams and payment fraud is increasing. Online consumers are exposed to a range of cybersecurity threats and fraud. This study aims to explore user behavior, fraud awareness, trust in e-commerce platforms, and experience with fraud and cyber security practices among e-commerce users. The research is quantitative descriptive research with 1,008 respondents selected by purposive sampling. Data were collected through a survey questionnaire and distributed via Google Forms and analyzed through descriptive statistics specifically weighted mean and percentage.

The results showed that respondents have a moderate level of awareness, trust and confidence on online fraud and cyber security practices. A lot of users took some basic security steps like checking out seller feedback and verifying payment information before they went ahead with transactions. Results, however, showed that some respondents were still vulnerable to scams due to low confidence in their ability to detect fraud and lack of cybersecurity awareness.

The study also develops a conceptual framework for fraud detection using machine learning. The proposed framework can be used in future applications to detect suspicious transactions and fraudulent behaviors using Logistic Regression, Random Forest and K Means Clustering. The proposed framework is not implemented or tested in this study and is presented as a proposed model for future development. The results underscore the need for improved fraud prevention strategies, heightened cybersecurity awareness and the potential of machine learning solutions to facilitate safer online transactions.

Keywords: E-Commerce Fraud; Payment Fraud; Order Scams; Cybersecurity Awareness; Machine Learning; Fraud Detection; Online Shopping Behavior; E-Commerce Security; Digital Transactions; Online Payment Systems; Consumer Trust; Cybercrime Prevention.

1.0. Introduction

The explosive growth of e-commerce has transformed the way people shop and how organizations do business. Online buying also opens the chance for order scams and payment fraud with its ease, availability and speedier payment procedures. Recent studies have shown that with the expansion of e-commerce platforms, the growth of fraudulent activities is also happening, harming the customers and sellers in terms of financial loss, destroying confidence and security difficulties. Mutemi and Bacao (2024) state that the increase in digital fraud is connected to the expansion of e-commerce, particularly since the Coronavirus Disease 2019 (COVID-19) epidemic, and the requirement for efficient anti-fraud strategies. (2025) observed that e-commerce fraud takes different forms such as false accounts, payment fraud, account takeover, bogus reviews, and promotional abuse. Order frauds and payment frauds are among the most important problems in e-commerce, as they are directly connected to the process of buying and selling. Scammers can generate fraudulent orders, leverage payment information they've stolen, abuse discounts, generate fake accounts or manipulate online transactions for their own benefit. According to Sánchez-Paniagua et al. (2025) the increase in e-commerce websites has provided a lot of opportunities for the

cybercriminals to create fake online stores and scams which can trick the customers. Singh (2021) also mentioned that the growing use of online banking, credit cards and debit cards has made the digital transactions prone to online frauds, phishing, illegal transactions and card-not-present frauds. Existing research explores the possibility of using machine learning as a tool for fraud detection; however, this study does not seek to design, train or use a machine learning model. Rather, it is concerned with offering a conceptual detection framework based on machine learning, based on the opinions, experiences and replies collected using a Google Forms survey. The objective is to learn about the major problems that users may encounter, the probable signs of fraud and the main characteristics of systems that can assist e-commerce platforms recognize or prevent suspicious orders and payment fraud. This allows the study to be more centered on framework design and user-based assessment than technical implementation. Traditional fraud detection techniques such as human verification, static rules and block lists are inadequate as fraud techniques are constantly evolving. (2025) Rule based and black-list based systems are restricted because of their reliance on reports, pre-specified variables and rules. Moreover, especially after the COVID-19 outbreak, there is a need for robust anti-fraud measures. (2025) commented that fraud detection in e-commerce is tough, as fraudulent behavior might be anonymous, changeable and difficult to differentiate from legitimate user activities. The results confirm the importance of a proposed framework that considers user behavior, transaction pattern, order detail and payment related warning indications as possible elements in fraud detection.

1.1. Study Objectives

General Objective

To assess the level of awareness, experiences, and vulnerability of consumers toward online payment fraud and order scams in e-commerce platforms using survey data and to evaluate existing fraud prevention measures based on respondents' perceptions.

Specific Objectives

1) To determine the level of awareness of respondents regarding online payment fraud and order scams.
2) To identify the most common types of scams and fraud experienced or witnessed by respondents.
3) To evaluate the effectiveness of existing fraud detection and prevention measures used by e-commerce platforms.
4) To assess the financial and digital literacy of respondents related to online transactions.
5) To investigate the factors that contribute to consumers' vulnerability to online fraud and deception.
6) To gather recommendations from respondents regarding improvements in user protection and fraud prevention measures.

1.2. Statement of the Problem

Most issues that arise in the current e-commerce system are those that often arise in the early phases of user-vendor interaction and the digital payment process. These issues include the following:

1. How reliable are the present e-commerce fraud protection strategies, and what level of cybersecurity knowledge do customers have while doing online transactions?
2. Does implementing advanced processes meant to identify suspicious activity such as confirming sellers and authenticating payments to make consumers less exposed to online scams?
3. How can a machine learning-based detection framework reduce financial failure rates in e-commerce platforms and detect fraudulent patterns?

1.3. Hypotheses of the Study

H1: Consumer level of cybersecurity awareness has a negative significant correlation with the tendency to experience online order scams and payment fraud.

H2: Perceived efficiency of conspicuous security features and automated fraud detection systems contribute significantly to increased customer trust in an e-commerce site.

H3: Customer behavior toward low-risk payment methods (e.g., Cash on Delivery) is significantly influenced by their past experiences of or exposure to e-commerce fraud.

1.4. Theoretical Background

Two main theoretical frameworks underpin this study: the Routine Activity Theory and the Protection Motivation Theory explain the behavior associated with cyber fraud and protection measures against it.

The Routine Activity Theory (RAT) was developed initially by criminologists to determine the occurrence of crime when three conditions are met: a motivated offender, a suitable target and lack of capable guardianship. In online environment, the offenders are the online fraudsters, the suitable targets are the internet users with lower digital literacy. Traditional, rule-based security mechanisms may fail as capable guardians due to the evolving nature of fraud. It provides the rationale of the importance of an adaptive Machine Learning based Detection Framework as a "capable guardian" and detects the anomalies of a transaction in real-time.

The Protection Motivation Theory (PMT) is applied to analyze consumers' behaviors in regard to threats in cyber space. It states that people are motivated to protect themselves when threat appraisal and coping appraisal of a situation is evaluated. Threat appraisal involves an individual's evaluation of the severity of online fraud and his/her individual vulnerability to this threat. Coping appraisal indicates how effective a security system/mechanism, e.g. Checking the reviews of the sellers, or selecting cash-on-delivery method, is believed to be in mitigating threats. PMT explains why users exhibit certain precautions to prevent the loss of funds. It further emphasizes the value of conspicuous security systems to elevate the users' coping appraisal and consequently their level of confidence toward the website.

2.0. Literature Review

While the advancement of e-commerce technology has been very helpful in making purchases of goods and services easier and more convenient, there has been an increase in the rate of fraud cases through e-commerce

technology. As indicated by Mutemi and Bacao (2024), the increase of e-commerce technology following the emergence of the Coronavirus Disease 2019 (COVID-19) has facilitated the growth of frauds in cyber space, resulting in losses on both the consumer and business ends. It is, therefore, safe to assume that order fraud and payment fraud are major issues within e-commerce.

Order scams and payment fraud can include fake accounts, payment fraud, account takeovers, fake reviews, misuse of promotions, phishing and similar fraudulent activities. The e-commerce fraud is difficult to detect because of the anonymity of the fraud on the virtual platform (Chen et al., 2025). They state that e-commerce fraud can be opportunistic deal-seeking, account takeover, payment fraud, fake accounts and fake reviews. The finding is relevant to this study where many online consumers may face fraud vendors, non-delivery of goods, unauthorized transactions and phishing when using e-commerce platforms. Consumers are increasingly using digital payment methods such as e-wallets, online banking and credit or debit cards, which has raised growing concern about online payment fraud. The growing popularity of e-commerce, online payment systems, digital banking and social networking platforms have made online payment systems attractive to fraudsters (Alrasheedi, 2025). The study further elaborated that the digital transactions may be vulnerable as the payments can be concluded without the physical presence of the account or cardholder. This shows that consumers need to be aware of the risks involved in online payments and must verify the transaction details before completing their purchases.

Although many studies have explored the potential of machine learning in improving fraud detection, these studies are used here as a theoretical foundation rather than a practical implementation. Machine learning and data mining methods are often used in fraud detection as they can detect patterns in e-commerce transactions (Mutemi and Bacao 2024). Chen et al. (2025) also surveyed the current literature on fraud detection, including rule-based, machine learning, user behavior analysis, and graph-based methods. In our study, however, we do not build, train, or test a machine learning model but propose a conceptual machine learning-based fraud detection approach that can be used as a reference for future system development based on survey findings. Digital literacy and consumer awareness are crucial to reducing susceptibility to online fraud. As Papasavva et al. (2025) pointed out online fraud impacts not only the emotional and psychological well-being of the victims but also their financial security. Their systematic evaluation also brought to light the fact that online fraud is continuously evolving because of the adaptation of fraudsters to new technologies and online opportunities. This underscores the importance of investigating consumers' confidence, experiences and awareness about suspicious transactions. Consumers may be more susceptible to unauthorized payment activities, phishing communications, and fake sellers if they possess inadequate comprehension of fraud indicators.

Table 1. Comparative Analysis of Fraud Detection and Security Strategies in E-Commerce Platforms

Feature	Traditional Approach	Machine Learning-Based Strategy	Impact on E-Commerce Security
Fraud Detection Method	Uses rule-based and manual verification systems.	Uses machine learning algorithms such as Logistic Regression, Random Forest, and K-Means Clustering.	Improves the accuracy and speed of fraud detection.

Transaction Monitoring	Transactions are checked after reports or complaints are received.	Real-time monitoring detects suspicious transactions automatically.	Reduces financial losses and prevents fraud earlier.
User Verification	Basic password authentication and manual account checking.	Multi-factor authentication and behavioral analysis are applied.	Strengthens account security and reduces unauthorized access.
Detection of Suspicious Activities	Limited to predefined fraud indicators and blacklist systems.	Learns transaction patterns and identifies anomalies dynamically.	Detects evolving fraud techniques more effectively.
System Scalability	Performance decreases during high transaction volumes.	Cloud-based and distributed systems support scalable operations.	Maintains system reliability and availability during peak usage.
Customer Trust and Security	Users rely mainly on seller reviews and manual checking.	Automated fraud detection and visible security measures increase confidence.	Enhances customer trust in online transactions.

3.0. Methodology

3.1. Research Design

This research used a quantitative descriptive research design to assess consumer awareness, trust, cybersecurity practices, and susceptibility to fraud in e-commerce websites and proposed a fraud detection framework based on machine learning to avoid order scams and payment frauds in online transactions. The data was collected from the online consumers who are actively using the e-commerce platform like Shopee, Lazada, Facebook Marketplace, and other digital shopping applications through purposive sampling to ensure the previous experience of the respondents in online shopping and digital payment transactions. The main research tool was a structured survey questionnaire comprising demographic profile, awareness of online fraud and payment scams, experiences of e-commerce fraud, cybersecurity practices, trust in online shopping platforms and evaluation of existing fraud prevention measures. The survey was distributed via online platforms like Google Forms and social media channels to reach a wider population of online consumers. The responses were analyzed using descriptive statistical tools such as frequency counts, percentages, weighted mean and methods of data interpretation to determine consumer behavior and fraud awareness levels. The proposed machine learning based fraud detection framework may help to identify suspicious online transactions and improve cybersecurity protection in digital commerce systems by using transaction patterns, user behavior analysis and fraud indicators. The researchers assured that all the information gathered was confidential and was used for academic purposes only. Participation in the study was voluntary with the informants being informed of the purpose of the study before answering the survey questionnaire.

3.2. Participants

This study utilized a quantitative-descriptive research design to evaluate consumer awareness, cybersecurity practices, trust, and fraud vulnerability in e-commerce platforms, and to propose a machine learning-based fraud detection framework to combat order scams and payment fraud. Data were obtained using purposive sampling from online consumers who actively use Shopee, Lazada and Facebook Marketplace. Data on fraud awareness,

online shopping behavior, cybersecurity practices and experiences of e-commerce fraud were collected using a structured survey questionnaire. The survey was distributed through Google Forms and social media platforms and the data collected were analyzed through frequency counts, percentages and weighted mean. All data collected were treated as confidential and used for academic purposes only.

3.3. Instrumentation

The major instrument used for data collection in this study is a well-constructed survey questionnaire consisting of 15 items that are designed to collect quantitative information regarding consumer awareness, cybersecurity practices, online shopping behavior, and experiences of e-commerce fraud. The questionnaire asked questions about things like awareness of fraud, confidence in e-commerce sites, security of payments and user experiences of online scams. The level of agreement and experiences of the respondents for each statement was measured by using a 5-point Likert scale which enabled the researchers to obtain data that was accurate, objective and statistically analyzable.

The questionnaire was prepared via Google Forms, to ease the collection and access of the data.

Table 2 presents the five-point Likert scale values and their corresponding interpretations used in analyzing the respondents' answers in the study.

Table 2. Five-Point Likert Scale Values Used for Interpreting Respondents' Answers in the Study.

Value		**Interpretation**	
1	Very Low	Strongly Disagree	Never
2	Low	Disagree	Rarely
3	Neutral	Sometimes	Not Sure
4	High	Agree	Often
5	Very High	Strongly Agree	Always

Table 3 presents the multiple-choice response options and their corresponding descriptions used in analyzing the respondents' answers regarding online shopping behavior, fraud awareness, and cybersecurity practices.

Table 3. Multiple-Choice Response Options and Corresponding Descriptions Used in Assessing Respondents' Online Shopping Behavior and Fraud Awareness.

Multiple-choice responses		
Yes	No	Maybe Questions

3.4. Data Collection Method

The responses were organized and subjected to statistical analysis after the data collection process was completed. Descriptive statistics such as frequency distribution, percentage, mean, and standard deviation were used to summarize the respondents' awareness, cybersecurity practices, online shopping behavior, and experiences with e-commerce fraud. Inferential statistical tools were also utilized to examine the relationships between consumer awareness, trust, cybersecurity practices, and vulnerability to online scams. The Pearson correlation coefficient

was used to determine the strength and direction of the relationships among the study variables, while multiple regression analysis was conducted to identify the significant factors influencing consumers' vulnerability to fraud and trust in e-commerce platforms. Through these analyses, the researchers were able to identify the factors that strongly affect online consumer security and fraud prevention in digital transactions.

3.5. Data Gathering Procedure

The researchers prepared and validated the survey questionnaire according to the objectives of the study. After the questionnaire was filled in, the Google Forms link was shared to targeted respondents via online platforms and social media channels. Collected responses were tabulated, checked and prepared for statistical analysis

3.6. Data Analysis

The data collected were analyzed using descriptive statistical methods, specifically:

Weighted Mean (WM)

$WM = \sum (f \times x) / N$

Where:

f = frequency of responses

x = Likert scale value

N = total number of respondents

Used for: Likert-scale responses Measuring level of agreement or frequency Percentage

Percentage = $f / N \times 100$

Used for: Multiple-choice responses Yes/No/Maybe questions

The results were presented in tables and interpreted according to the objectives of the study.

Table 4 presents the mean score ranges and their corresponding descriptive interpretations used in analyzing the respondents' perceptions, awareness, and experiences related to e-commerce fraud and online transactions.

Table 4. Mean Score Ranges and Descriptive Interpretations Used in Evaluating Respondents' Awareness, Experiences, and Cybersecurity Practices in E-Commerce Platforms.

Range	Interpretation
1.00 – 1.80	Very Low
1.81 – 2.60	Low
2.61 – 3.40	Neutral
3.41 – 4.20	High
4.21 – 5.00	Very High

3.7. Proposed Machine Learning-Based Fraud Detection Framework

The work proposes a conceptual machine learning based fraud detection framework to effectively address the evolving nature of threats in online transactions, particularly to detect and combat order scams and payment fraud

in e-commerce platforms. This framework is based on behavioral patterns, transaction habits, and real-world fraud experiences pulled directly from the study's survey data, rather than traditional static rule-based systems. The proposed model combines three different machine learning algorithms to provide multi-layered approach for threat detection. Firstly, we introduce Logistic Regression, a simple binary classifier that attempts to classify incoming transactions as only fraudulent or legitimate using previous variables. Second, a Random Forest algorithm is also included to cover more sophisticated threat vectors. This strategy, based on a collection of decision trees, can detect highly complex and non-linear fraud patterns that can be overlooked by a single algorithmic model. At last, K-Means Clustering is used as an unsupervised learning technique to identify anomalies by clustering normal user behavior and automatically flagging abnormal, outlier activities that deviate from the norm. It is important to note that the user data were analyzed in detail using descriptive statistical methods, especially weighted means and percentages, to justify the need for this system, but the proposed machine learning techniques are still conceptual. This framework is a high-level architecture design that will guide the future implementation and technical deployment.

3.8. Ethical Considerations

Since financial transactions and cybersecurity experiences are sensitive issues, the researchers made sure to adhere strictly to all rigorous ethical standards and data privacy protocols throughout the entire study. First and foremost, the participation in the research was voluntary in its entirety with an express focus on gaining informed consent. Before taking part in the survey all respondents were fully informed of the exact purpose of the research, the precise type of data being collected and the precise manner in which their responses would be used to draw the study's conclusions. Strict confidentiality was maintained to ensure high levels of data privacy. At no point in the data gathering process were Personally Identifiable Information (PII) or sensitive financial credentials required, requested or disclosed. Furthermore, to guarantee complete anonymity and safety of the participants, all collected responses were stored, treated and reported only in an aggregated, statistical form. This ensured that no individual respondent could be traced or identified through the published findings.

4.0. Results and Discussion

The chapter presents the results of the study and their interpretation based on the data collected. The paper also discusses the implications of the results with respect to online fraud awareness and the proposed Machine Learning framework.

4.1. Online Shopping Behavior

Table 5 presents the frequency of online shopping activities of respondents in various e-commerce platforms used for digital transactions and online purchases.

Table 5. Frequency of Online Shopping Activities of Respondents in E-Commerce Platforms

Indicator	Mean	Interpretation
Frequency of Online Shopping	3.34	Moderate

Figure 1 illustrates the preferred payment methods used by respondents during online transactions in e-commerce platforms.

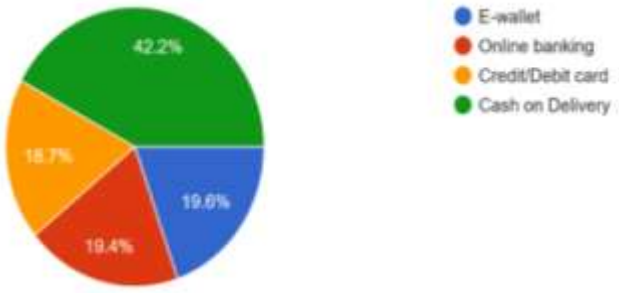

Figure 1. Distribution of Preferred Payment Methods Used by Respondents during Online Transactions in E-Commerce Platforms.

This shows that the level of frequency of online shopping by the participants is moderately high (WM = 3.34), meaning that they sometimes conduct business online. Looking at the payment method used by respondents, Cash on Delivery (COD) takes the lead, accounting for 42.2% of all payments, while the other two preferred methods are e-wallets and online banking. This indicates that respondents prefer safe payment methods online.

4.2. Awareness of Online Fraud

Table 6 presents the frequency of respondents' exposure to online fraud and payment scam incidents encountered while using e-commerce platforms and digital payment services.

Table 6. Frequency of Respondents' Exposure to Online Fraud and Payment Scam Incidents in E-Commerce Platforms

Indicator	Mean	Interpretation
Frequency of Hearing About Fraud Incidents	3.24	Moderate

Figure 2 illustrates the level of awareness of respondents regarding online fraud and payment scams encountered in e-commerce platforms and digital transactions.

Figure 2. Level of Awareness of Respondents Regarding Online Fraud and Payment Scams in E-Commerce Platforms**.**

Awareness of fraud cases on the Internet has been found at an average rate of 3.24, which suggests that the respondents know about fraud cases but lack thorough knowledge of them. Such an awareness rate shows that

people are aware of the presence of fraud cases but require more knowledge in this regard.4.3 Trust in E-Commerce Websites.

4.3. Trust in E-Commerce Platforms

Table 7 presents the level of consumer trust in online shopping platforms and digital transactions based on the respondents' experiences and perceptions regarding online security and fraud prevention.

Table 7. Level of Consumer Trust in Online Shopping Platforms and Digital Transactions in E-Commerce Websites

Indicator	Mean	Interpretation
Trust in Online Shopping Platforms	3.14	Moderate

The results reveal a moderate level of trust in e-commerce platforms (WM = 3.14), indicating that respondents are cautious when engaging in online transactions. This suggests that concerns about fraud and security issues may influence user confidence, highlighting the importance of improving platform reliability and security measures.

4.4. Experience with Fraud

Figure 3 illustrates the different types of online fraud and payment scams experienced by respondents while using e-commerce platforms and digital payment services.

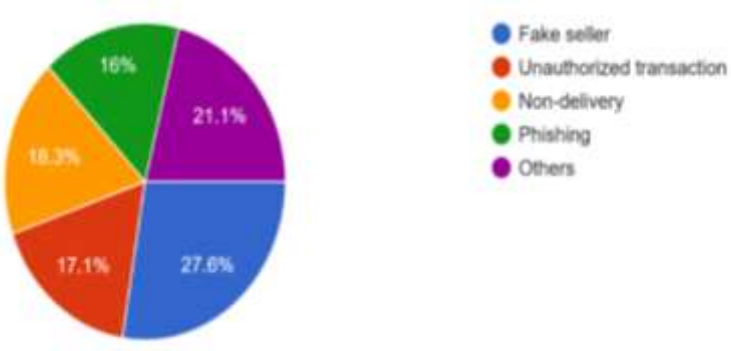

Figure 3. Distribution of Types of Online Fraud and Payment Scams Experienced by Respondents

Table 8 presents the respondents' experiences with online fraud and payment scams encountered while conducting transactions through e-commerce platforms

Table 8. Respondents' Experiences with Online Fraud and Payment Scams in E-Commerce Platforms

Indicator	Mean	Interpretation
Effect of fraud on Willingness	3.24	Moderate

The findings indicate that the problem of fake sellers (27.6%) is the most experienced case of fraud, whereas non-delivery and fraudulent transactions follow. The significant effect of fraud on willingness (WM = 3.24) suggests that even though fraud experiences affect user's behavior, the users still continue doing their online shopping very cautiously.

4.5. Perception of Fraud Detection Systems

Table 9 presents the respondents' perceptions regarding the effectiveness of fraud detection systems used in e-commerce platforms and online transactions.

Table 9. Respondents' Perception of Fraud Detection Systems Used in E-Commerce Platforms and Online Transactions.

Indicator	Mean	Interpretation
Security Features Increase Trust	3.20	Moderate

Figure 4 illustrates the impact of security features on consumer trust and protection while conducting transactions in e-commerce platforms.

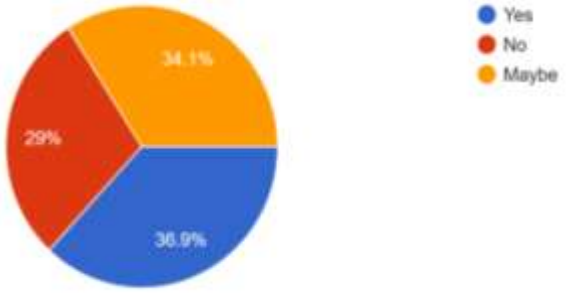

Figure 4. Impact of Security Features on Consumer Trust and Protection in E-Commerce Platforms.

Figure 5 illustrates the level of user confidence in automated fraud detection systems used to enhance security during online transactions.

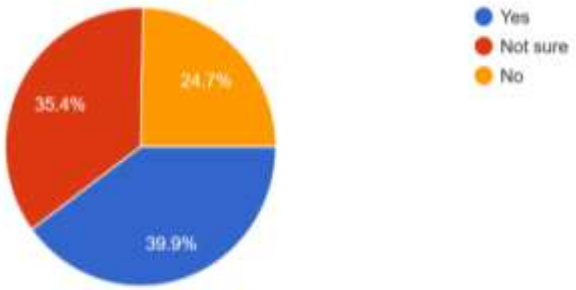

Figure 5. Level of User Confidence in Automated Fraud Detection Systems Used in Online Transactions.

These results suggest a fair belief about fraud detection technology (WM = 3.20). This implies that the majority of users perceive a positive impact of security technology on increasing their trust towards online transactions. However, as seen from the statistics, 36.9% and 39.9% of users were sure about their positive attitude, whereas a considerable number of users felt unsure.

4.6. Cybersecurity Awareness and Confidence

Table 10 presents the respondents' level of cybersecurity awareness and confidence in protecting their online transactions from fraud and security threats.

Table 10. Respondents' Cybersecurity Awareness and Confidence in Protecting Online Transactions

Indicator	Mean	Interpretation
Checking Seller Review	3.53	High
Verifying Payment Details	3.48	High
Confidence in Identifying Suspicious Transaction	2.61	Moderate

Figure 6 illustrates the respondents' formal education or training related to online security and cybersecurity awareness in digital transactions and e-commerce platforms.

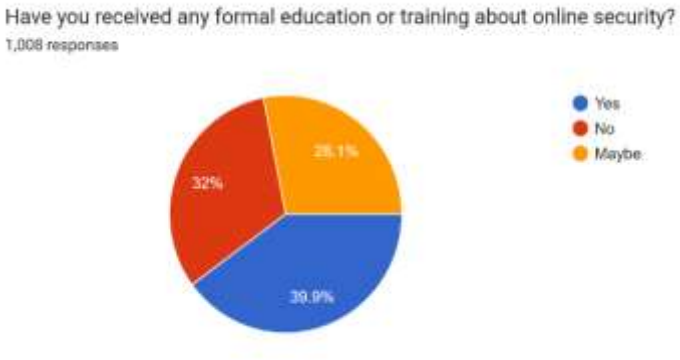

Figure 6. Respondents' Formal Education or Training Related to Online Security and Cybersecurity Awareness

The finding from the analysis shows that respondents have high security practices, as indicated by their frequent review of reviews done by sellers (WM=3.53) and payment information verification (WM=3.48). However, the confidence of these respondents towards identifying fraudulent activities is relatively low (WM=2.61). It is clear, therefore, that even though the respondents have high cybersecurity practices, they are still vulnerable to fraudulent activities.

Furthermore, it has been found that there are quite a few respondents who have low confidence in detecting fraudulent transactions.

5.0. Conclusion and Recommendation

5.1. Summary of Findings

The study presented a holistic analysis of the interlinked aspects concerning user behaviour, prior knowledge, platform trust, personal experiences with fraud, existing cybersecurity practices with regard to order scams and payment frauds on e-commerce platforms. The data collected shows that the respondents were to some extent aware of online fraud. This suggests that while consumers are aware of the existence of online scams, they are not knowledgeable or prepared to fully protect themselves against sophisticated fraudulent practices. As a result, e-commerce platforms had a moderate level of confidence, indicating that consumers are generally cautious and wary about engaging in online transactions. For example, the data revealed that the most common type of fraud that the participants experienced was "fake seller" frauds. This implies that seller deception is a persistent and serious threat to the integrity of online shopping ecosystems. The most common active cybersecurity measures users said

they took were basic checks such as regularly checking seller ratings and confirming payment details before a purchase. Despite these basic safety measures, users report only moderate confidence in their ability to detect fraud and identify suspicious activity, creating a key vulnerability gap.

5.2. Conclusions

The synthesized results conclude that despite exercising careful online shopping habits and basic cybersecurity precautions, e-commerce consumers are highly vulnerable to online scams and payment fraud. The general average levels of awareness, trust and confidence can be directly interpreted to mean that the general users are currently not equipped with the skill set required to consistently detect and avoid sophisticated fraudulent schemes during online transactions. The high frequency of such fake seller scams also indicates that there is an urgent and significant need for systemic measures, and that the existing verification system is not working. This reality requires a much stronger fraud prevention infrastructure and targeted cybersecurity education for both users and platform administrators. Finally, the study concludes that traditional rule-based security is not enough and thus proposes a conceptual machine learning based framework. This model is an important future direction for automatic detection of anomalous transactions and fraudulent behavior in complex e-commerce environments. The focus of this particular study was on the conceptualization of the framework, not its technical implementation. It provides a strong foundational blueprint, however, for future studies to build upon in order to develop dynamic, AI-driven security systems.

5.3. Recommendations

Based on the findings of this study, the following is the full list of recommendations suggested to improve the security and reliability of the e-commerce landscape:

For users of E-Commerce:

1. Users need to be more aware of the changing environment of online scams. They want to learn how to spot the tell-tale signs of suspicious behavior from bad actors selling products, and stick to safe online transaction practices to dramatically reduce the likelihood of being targeted.
2. Another reason why online shopping is becoming so popular is the convenience. We highly recommend that consumers research the legitimacy of the vendor, review the reviews of the item for authenticity and verify all payment information before making a purchase.
3. Extra Care Users should also exercise extra care when sharing sensitive financial and personal information through third party communication channels, unverified sellers and suspicious websites without appropriate security certificates.
4. Consumers have a role to play to better secure their own accounts and transactions. And this means using strong and different pass-words for different platforms. It also means turning on two-factor authentication (2FA) if possible and only using safe and verifiable methods of payment.

For System Admins and E-Commerce Sites:

1. It is necessary for e-commerce platforms to revise and perfect the systems of seller verification in time to protect the validity of the platforms. This translates into improved on-boarding processes to significantly reduce the number of fake vendors and fraudulent deals.
2. Communicate embedded security features and fraud prevention measures to platform administrators in a strategic and effective manner to increase visibility and ensure consumer confidence and safety.
3. It is important to develop permanent and real-time monitoring and detection systems (such as the proposed machine learning framework) that can automatically detect suspicious actions, flag anomalous patterns and intercept probable attempts of fraud before they affect the consumer.
4. Proactively enable users. E-commerce platforms need to continually put out focused security awareness notifications and real time fraud alerts that will effectively teach users to recognize on their own dangerous transactions and new scam tactics.
5. The ever-changing nature of cyber threats requires continued reassessment and stress-testing of cybersecurity policies of the organization and platform security mechanisms. It also requires dynamic updating of such policies by e-commerce administrators to ensure long-term reliability and secure architecture of the platform.

For Future researchers

1. Future studies may implement and test the proposed machine learning framework using real-time transaction datasets.
2. Researchers may compare the effectiveness of different machine learning algorithms in detecting e-commerce fraud.
3. Future systems may integrate artificial intelligence-based behavioral analytics for improved fraud prediction.
4. Researchers may conduct studies involving larger and more diverse respondent populations.
5. Future work may evaluate the effectiveness of cybersecurity awareness programs among online consumers.
6. Future researchers may develop mobile-based fraud alert systems for safer digital transactions.

Declarations

Source of Funding

This research did not benefit from grant from any non-profit, public or commercial funding agency.

Competing Interests Statement

The authors have declared that no competing financial, professional or personal interests exist.

Consent for publication

All the authors contributed to the manuscript and consented to the publication of this research work.

Availability of data and material

Supplementary information such as the raw files of the data gathering and data analysis are available from the authors upon reasonable request.

Authors' Contributions

All authors contributed equally to the conceptualization, data gathering, analysis, writing, editing, and revision of the manuscript.

Informed Consent

Informed consent was obtained from all respondents prior to participation in the study.

Institutional Review Board Statement

Not Applicable.

Ethical Approval

The study followed ethical research standards and ensured confidentiality, anonymity, and voluntary participation.

Declaration of Artificial Intelligence

Artificial intelligence tools were used only for grammar enhancement and language refinement. All analyses and interpretations were conducted by the researchers.

Acknowledgments

The researchers would like to give sincere thanks to the University of Science and Technology of Southern Philippines – Oroquieta for providing the academic platform and support needed for the study. We are thankful to the faculty members of the Department of Information Technology for their continuous guidance, useful insights and encouragement throughout the research process.

We would like to thank very specially and sincerely the 1008 e-commerce users who have willingly participated in the data gathering phase. We could not have done this study without their time, cooperation and honest answers. The members of the research team also deserve much gratitude for their unwavering dedication and teamwork that helped bring this manuscript to completion.

The authors also want to express their deepest gratitude to their adviser Mr. Ginbert A. Fernandez for his excellent mentorship, constant support and high standards. His guidance always motivated the researchers to put their best efforts and successfully deal with the intricacies of this study.

In closing the authors wish to express their gratitude to their families, friends and loved ones for their unwavering moral support, patience and understanding throughout this academic endeavor.

References

[1] Sánchez-Paniagua, M., Fidalgo, E., Alegre, E., & Jáñez-Martino, F. (2026). Fraud detection in e-commerce: A comparative analysis of features to enhance machine learning models. Electronic Commerce Research, 26(1): 2467–2502. https://doi.org/10.1007/s10660-025-10029-9.

[2] Papasavva, A., Lundrigan, S., Lowther, E., Johnson, S., Mariconti, E., & Tuptuk, N. (2025). Applications of AI-based models for online fraud detection and analysis. Crime Science, 14(7): 1–18. https://doi.org/10.1186/s40163-025-00248-8.

[3] Zhang, Z., Yin, H., Rao, S.X., Yan, X., Wang, Z., Liang, W., Zhao, Y., & Shan, Y. (2025). Identifying e-commerce fraud through user behavior data: Observations and insights. Data Science and Engineering, 10(1): 24–39. https://doi.org/10.1007/s41019-024-00275-6.

[4] Rao, S.X., Jiawei, J., Han, Z., & Yin, H. (2025). Fraud detection in e-commerce: A systematic review of transaction risk prevention. IntechOpen, 1(1): 1–18. https://doi.org/10.5772/intechopen.1009640.

[5] Swetha, N., & Prasanna, S.L. (2025). Adaptive fraud detection in multi-participant e-commerce using process mining and machine learning. International Journal of Engineering Research and Science and Technology, 21(2): 892–902. https://doi.org/10.62643/ijerst.2025.v21.i2.pp892-902.

[6] Zhai, J. (2025). Automatic identification method for fraudulent users on e-commerce websites based on Random Forest algorithm. Journal of Computational Methods in Sciences and Engineering, 25(2): 1147–1154. https://doi.org/10.1177/14727978241295575.

[7] Farsi, S., & Chowdhury, M. (2025). EcomFraudEX: An explainable machine learning framework for victim-centric and dual-sided fraud incident classification in e-commerce. EAI Endorsed Transactions on Scalable Information Systems, 12(2): 1–15. https://doi.org/10.4108/eetsis.6789.

[8] Kumar, A.A., & Raju, S.H. (2025). An accurate fraud source path identification using integration of graphical neural networks, long-short term memories, and XGBoost. International Journal of Safety and Security Engineering, 15(11): 2343–2352. https://doi.org/10.18280/ijsse.151114.

[9] Li, X., Peng, Y., Sun, X., Duan, Y., Fang, Z., & Tang, T. (2025). Unsupervised detection of fraudulent transactions in e-commerce using contrastive learning. arXiv Preprint. https://arxiv.org/abs/2503.18841.

[10] Luo, R., Wang, N., & Zhu, X. (2025). Fraud detection and risk assessment of online payment transactions on e-commerce platforms based on LLM and GCN frameworks. arXiv Preprint. https://arxiv.org/abs/2509.09928.

[11] George, M.Z.H., Alam, M.K., & Hasan, M.T. (2025). Machine learning for fraud detection in digital banking: A systematic literature review. arXiv Preprint. https://arxiv.org/abs/2510.05167.

[12] Tax, N., de Vries, K.J., de Jong, M., Dosoula, N., van den Akker, B., Smith, J., Thuong, O., & Bernardi, L. (2021). Machine learning for fraud detection in e-commerce: A research agenda. arXiv Preprint. https://arxiv.org/abs/2107.01979.

[13] Weng, H., Li, Z., Ji, S., Chu, C., Lu, H., Du, T., & He, Q. (2018). Online e-commerce fraud: A large-scale detection and analysis. In Proceedings of the IEEE International Conference on Data Engineering, Pages 1441–1452, IEEE. https://doi.org/10.1109/ICDE.2018.00162.

[14] Ali, M.A., Azad, M.A., Parreno Centeno, M., Hao, F., & van Moorsel, A. (2019). Consumer-facing technology fraud: Economics, attack methods and potential solutions. Future Generation Computer Systems, 100: 408–427. https://doi.org/10.1016/j.future.2019.03.041.

[15] IBM Security (2024). Cost of a data breach report 2024. IBM Corporation.

[16] European Union Agency for Cybersecurity (2023). Threat landscape for phishing attacks. ENISA Publications. https://www.enisa.europa.eu/publications.

[17] National Institute of Standards and Technology (2023). Digital identity guidelines and multi-factor authentication standards. https://pages.nist.gov/800-63-3/.

[18] Organisation for Economic Co-operation and Development (2023). E-commerce challenges and digital fraud prevention. OECD Publishing. https://www.oecd.org/digital/.

[19] PCI Security Standards Council (2025). Payment card industry data security standards version 5.0. https://www.pcisecuritystandards.org/.

[20] Visa Inc. (2024). Digital payment security trends and fraud prevention. https://usa.visa.com/run-your-business/small-business-tools/payment-security.html.

[21] Mastercard Research (2023). Tokenization and encryption technologies in online payment systems. https://www.mastercard.us/en-us/business/overview/safety-and-security.html.

[22] Microsoft Security (2024). Artificial intelligence for fraud detection and cybersecurity. https://www.microsoft.com/security.

[23] Google Research (2023). Machine learning methods for anomaly detection in online payments. https://research.google/pubs/.

[24] Kaspersky (2025). Cyberthreat report on digital payment fraud. https://www.kaspersky.com/resource-center.

[25] McKinsey and Company (2023). Consumer trust and digital commerce security trends. https://www.mckinsey.com/capabilities/mckinsey-digital.

[26] World Economic Forum (2024). Global cybersecurity outlook 2024. https://www.weforum.org/reports/global-cybersecurity-outlook-2024/.

[27] Mendonça, R., Salazar, A., & Martinez, E. (2025). Graph-based deep learning for e-commerce fraud detection. Journal of Advances in Engineering and Technology, 2(1): 1–12. https://doi.org/10.62177/jaet.v2i1.211.

[28] Authors Unknown (2025). Towards effective and robust bank fraud detection thanks to machine learning. Procedia Computer Science, 265: 25–32. https://doi.org/10.1016/j.procs.2025.07.152.

[29] Juniper Research (2024). Online payment fraud: Emerging threats, segment analysis and market forecast 2023–2028. https://www.juniperresearch.com.

[30] Statista (2024). Retail e-commerce sales worldwide from 2014 to 2027. https://www.statista.com/statistics/379046/worldwide-retail-e-commerce-sales/.

[31] Mutemi, A., & Bação, F. (2024). E-commerce fraud detection based on machine learning techniques: Systematic literature review. Big Data Mining and Analytics, 7(2): 419–444. https://doi.org/10.26599/bdma.2023.9020023.

[32] Zhai, J. (2025). Automatic identification method for fraudulent users on e-commerce websites based on Random Forest algorithm. Journal of Computational Methods in Sciences and Engineering, 25(2): 1147–1154. https://doi.org/10.1177/14727978241295575.

[33] Tang, S., & Wong, R.K. (2026). Adaptive fraud detection on e-commerce platforms. Frontiers in Artificial Intelligence and Applications, 395: 333–340. https://doi.org/10.3233/faia240788.

[34] Mutemi, A., & Bação, F. (2023). A numeric-based machine learning design for detecting organized retail fraud in digital marketplaces. Scientific Reports, 13: 12499. https://doi.org/10.1038/s41598-023-38304-5.

[35] Zhao, W., & Liu, X. (2024). Detection of e-commerce fraud review via self-paced graph contrast learning. The Computer Journal, 67(6): 2054–2068. https://doi.org/10.1093/comjnl/bxae010.

[36] Damayanti, R., & Adrianto, Z. (2023). Machine learning for e-commerce fraud detection. Jurnal Riset Akuntansi dan Bisnis Airlangga, 8(2): 1450–1467. https://doi.org/10.20473/jraba.v8i2.48559.

[37] Lokanan, M.E., & Maddhesia, V. (2025). Supply chain fraud prediction with machine learning and artificial intelligence. International Journal of Production Research, 63(1): 286–313. https://doi.org/10.1080/00207543.2024.2361434.

[38] Doytshman, C., et al. (2023). FRAUDability: Estimating users' susceptibility to financial fraud using adversarial machine learning. ArXiv Preprint. https://arxiv.org/abs/2312.01200.

[39] Chen, C., et al. (2020). InfDetect: A large-scale graph-based fraud detection system for e-commerce insurance. ArXiv Preprint. https://arxiv.org/abs/2003.02833.

[40] Tax, N., et al. (2021). Machine learning for fraud detection in e-commerce: A research agenda. ArXiv Preprint. https://arxiv.org/abs/2107.01979.

[41] Luo, R., Wang, N., & Zhu, X. (2025). Fraud detection and risk assessment using LLM frameworks for online payment transactions on e-commerce platforms. ArXiv Preprint. https://arxiv.org/abs/2509.09928.

[42] Bitaab, M., et al. (2023). Beyond phish: Detecting fraudulent e-commerce websites at scale. In IEEE Symposium on Security and Privacy, Pages 2566–2583, IEEE. https://doi.org/10.1109/SP46215.2023.10179461.

[43] Rodrigues, V.F., et al. (2022). Fraud detection and prevention in e-commerce: A systematic literature review. Electronic Commerce Research and Applications, 56: 101207. https://doi.org/10.1016/j.elerap.2022.101207.

[44] Liu, Y., et al. (2023). Synthetic identity fraud in digital finance. Expert Systems with Applications, 213: 118946. https://doi.org/10.1016/j.eswa.2022.118946.

[45] Ryman-Tubb, N.F., et al. (2018). AI and ML in payment card fraud detection. Engineering Applications of Artificial Intelligence, 76: 130–157. https://doi.org/10.1016/j.engappai.2018.07.008.

[46] Weng, H., et al. (2018). Large-scale e-commerce fraud detection. In IEEE International Conference on Data Engineering, Pages 1441–1452, IEEE. https://doi.org/10.1109/icde.2018.00162.

[47] Wu, K., et al. (2018). Identifying counterfeit websites using ML. In International Conference on Internet and e-Business Systems, Pages 321–324, ACM. https://doi.org/10.1145/3282373.3282407.

[48] Zhang, X., et al. (2023). ML techniques for e-commerce research. Journal of Theoretical and Applied Electronic Commerce Research, 18(4): 2188–2216. https://doi.org/10.3390/jtaer18040110.

[49] He, H., & Garcia, E.A. (2009). Learning from imbalanced data. IEEE Transactions on Knowledge and Data Engineering, 21(9): 1263–1284. https://doi.org/10.1109/tkde.2008.239.

[50] Effective fraud detection in e-commerce using ML and big data analytics. (2024). Measurement: Sensors, 33: 101138. https://doi.org/10.1016/j.measen.2024.101138.